RSAC 2025 Conference

Many Voices.
One Community.

SESSION ID: FRP-M02

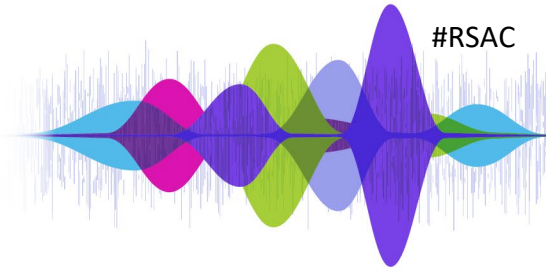
Boxing in the Bad Guys: Introducing the Fraud Kill Chain

Senan Moloney

Global Head of Cybercrime and Cyber Fraud Fusion
Barclays
linkedin.com/in/senan-moloney-9600053b

Eward Driehuis

VP of Fraud Engineering
ThreatFabric
linkedin.com/in/ewarddriehuis



Disclaimer

Presentations are intended for educational purposes only and do not replace independent professional judgment. Statements of fact and opinions expressed are those of the presenters individually and, unless expressly stated to the contrary, are not the opinion or position of RSA Conference LLC or any other co-sponsors. RSA Conference LLC does not endorse or approve, and assumes no responsibility for, the content, accuracy or completeness of the information presented.

Attendees should note that sessions may be audio- or video-recorded and may be published in various media, including print, audio and video formats without further notice. The presentation template and any media capture are subject to copyright protection.

© 2025 RSA Conference LLC or its affiliates. The RSAC and RSAC CONFERENCE logos and other trademarks are proprietary. All rights reserved.

Chasing Impossible Spends

Unravelling a ball of yarn

- We got a call about “impossible spends”
- There was existing research about NFSkate targeting ATMs in Eastern Europe
- Mobile involvement suspected
- When we shared our findings the impact the yarn started to unravel

2 Cyber Pros moved to Fraud Prevention

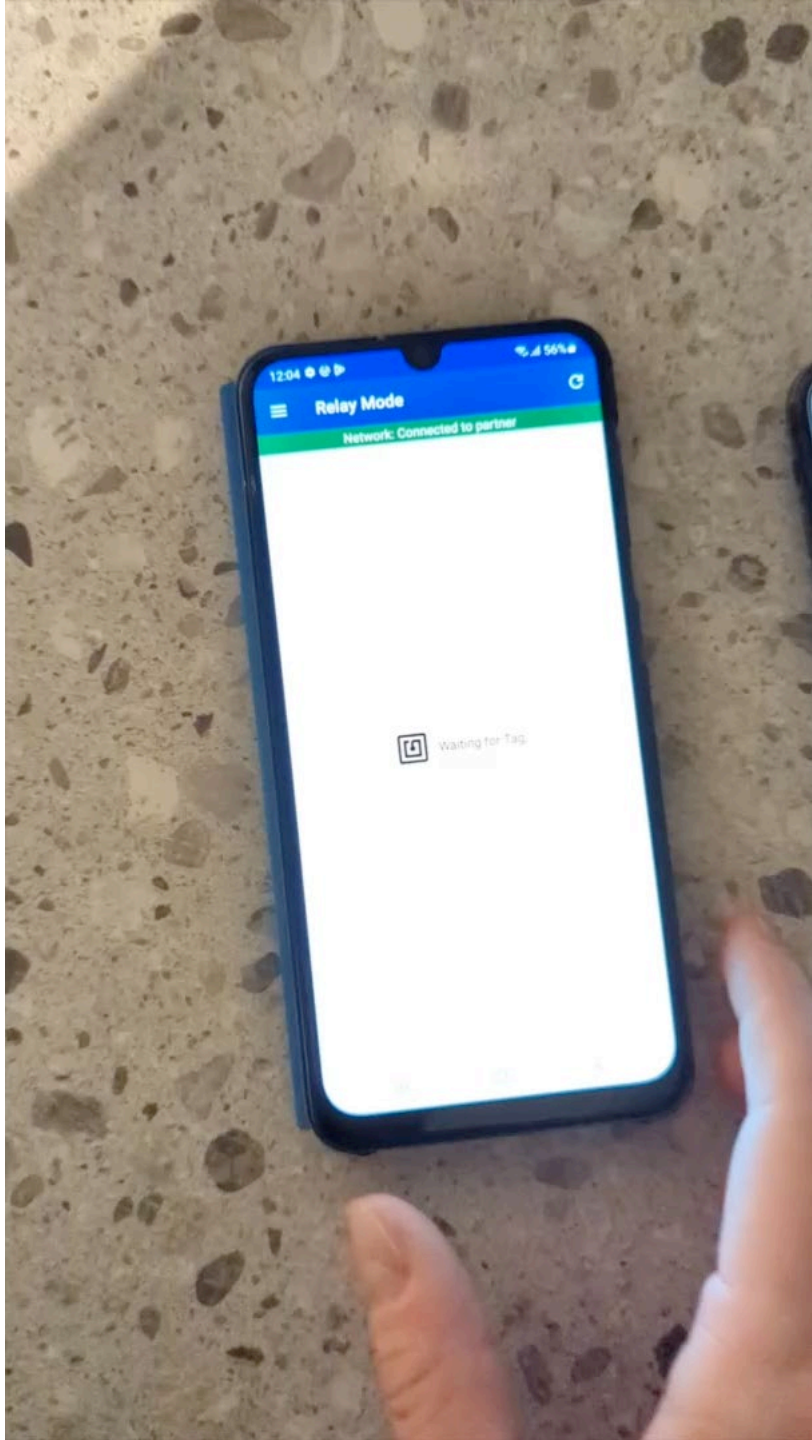
Senan Moloney

Eward Driehuis

Ghost Tap PoC

Demonstration

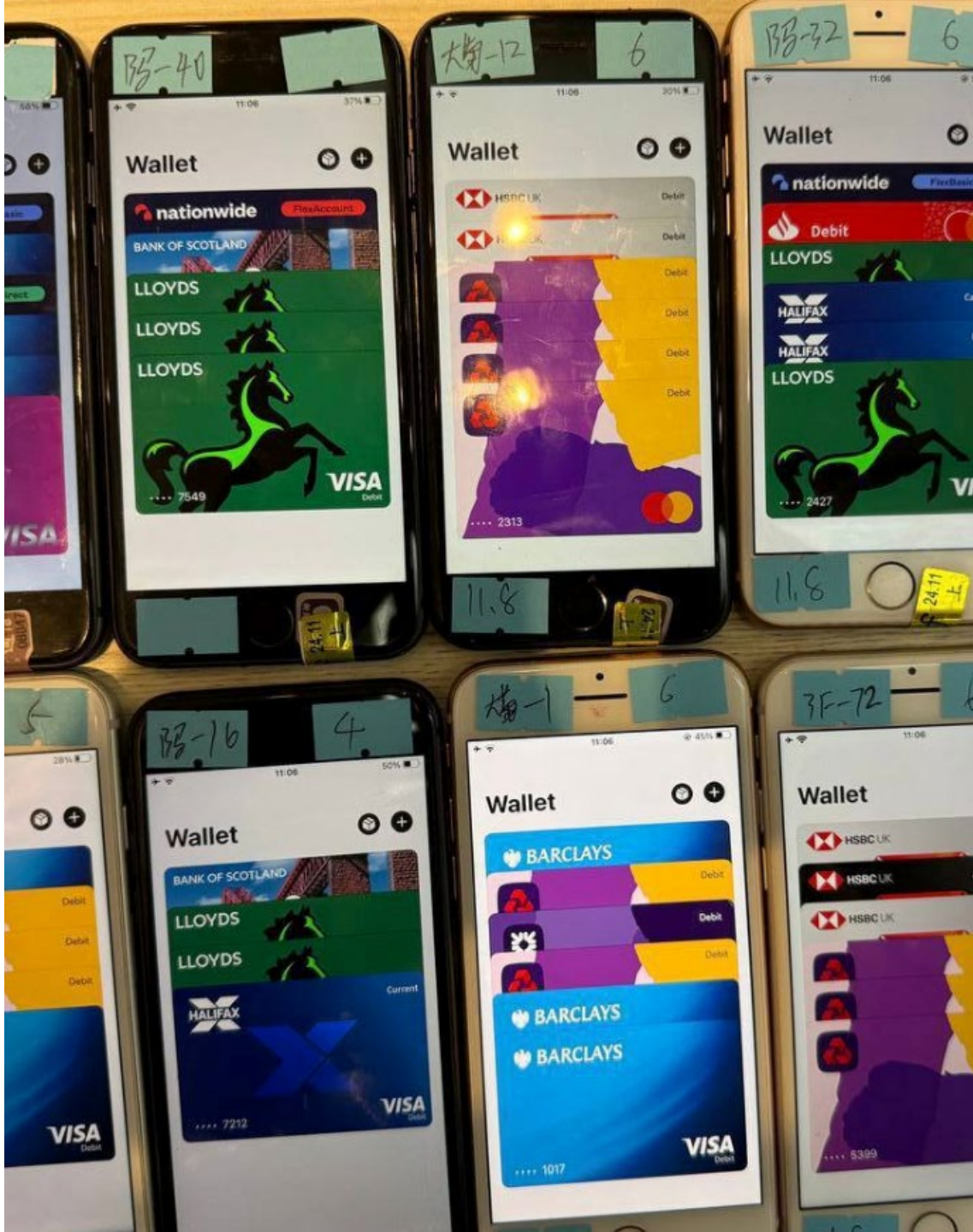
- MTI analysts built a proof of concept
- Using publicly available NFC Proxy code
- Same one used by underground actors
- Attempted to proxy Apple Pay payment for a can of Coke – success!
- New information about sightings in the UK, Eastern Europe and other parts of the world
- Criminals selling NFC relays in Underground forums as a cash-out method



Warnings lead to sharing

And understanding the bigger picture

- [TIE INTO Barclays Research].
- Other banks and researchers started contributing information
- NFC Relays one of several cash-out methods
- Others involve “Carding Gangs attributed to Chinese speaking actors
- Pre-provisioned cards on (stolen) phones



Many were aware, working on parts of the puzzle, or following different threads in ball of yarn...

Industry Concern

- Many different MO's including Selling Pre-Provisioned Cards in wallets on phones
- Many different FI's, other pieces of research coming together
- This proved the need to speak the same vocabulary
- Hence the need for the Fraud Kill Chain

Topology & Common Vocabulary

Attack TTPs & Mitigation Controls

- Let's look at the topology and how NFC Relay / Carding fits into this
- From NFSkate to POS NFC Cashouts
- Mapping TTPs
- Offering a way to identify gaps

Why a Fraud Kill Chain?

- And not something other like ATT&CK?
- Technical & behavioral manipulation
- Allow for non-technical / behavioral / Financial TTPs

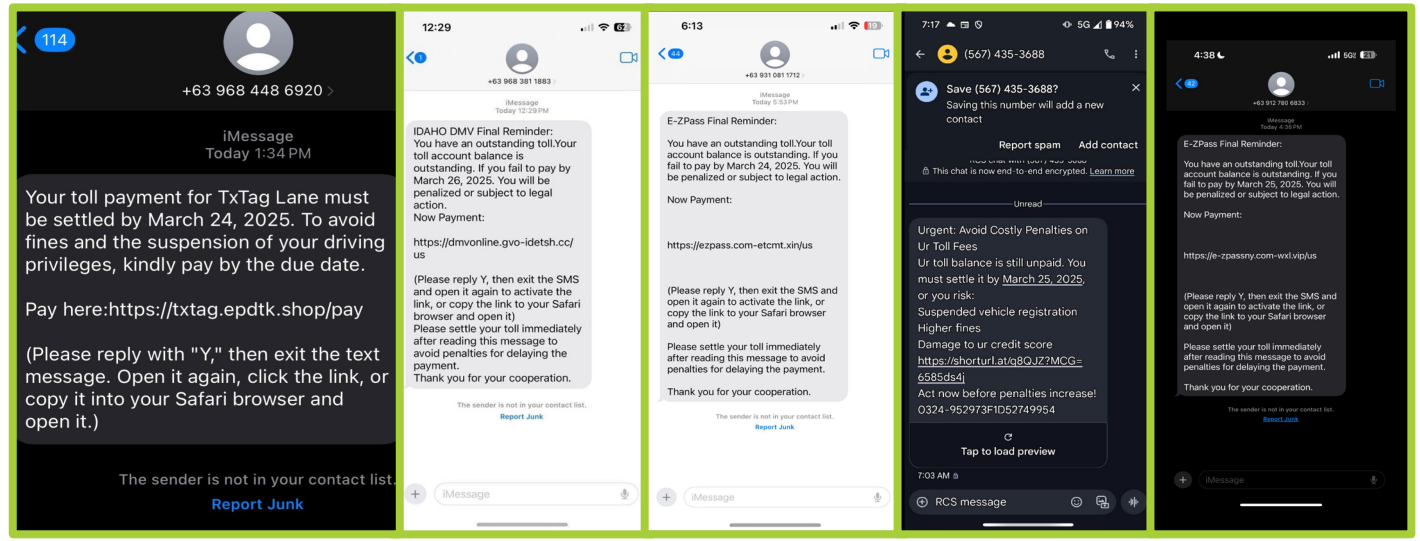
Overview of the Fraud Kill Chain

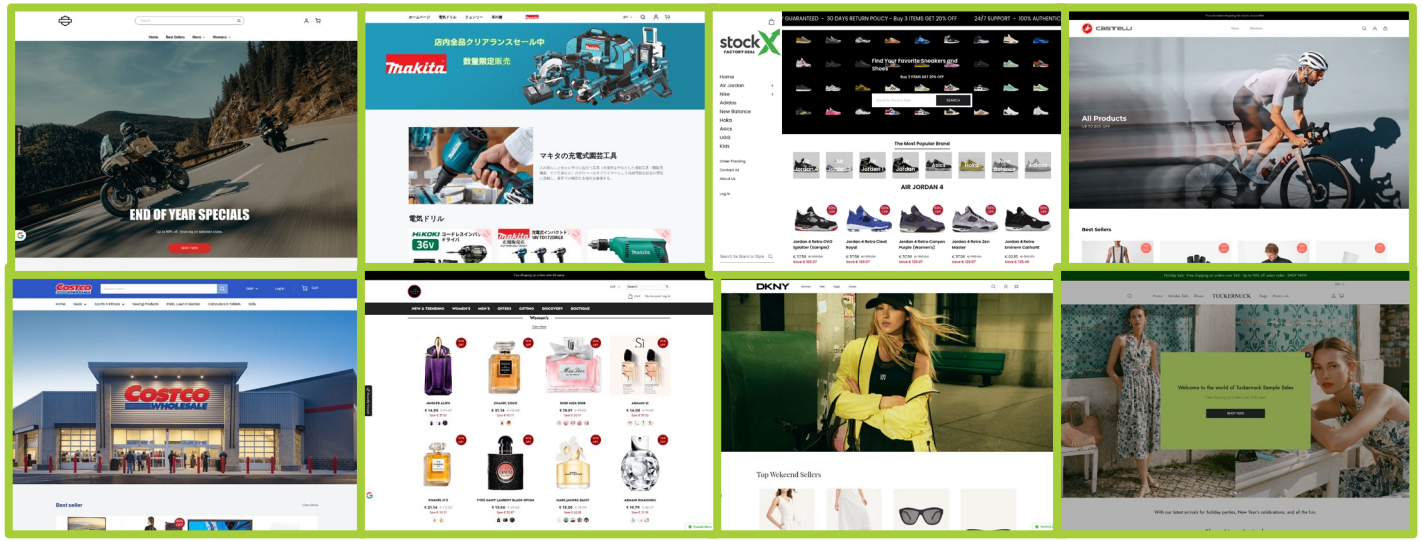
Digital Wallet Attacks: Preparation of the MOs

Reconnaissance	Resource Development	Psychological Manipulation	Faux Communications	Credential Compromise	Account Access	Authorization Compromise	Fraud Event	Monetization	Money Laundering
SMS Intercept	Acquire Infrastructure	Romance	Phishing	Keyloggers	Device Compromise	Location Spoofing	Victim Transfer	Cashout	Resale of Goods
Bots	Compromise Infrastructure	Impersonation	Spearphishing	Screen Capture	Insiders	Virtual Phone	Account Takeover	Subscriptions	Crypto Mixers
Malware	Social Networks Accounts	Accessibility Permissions	Smishing	SMS Intercept	Cloned Devices	Voice Changers	P2P Transfers	ATM Withdrawal	
Personal Info	Infected POS	Fake Loan Requests	Vishing	Card Dump Captures	Brute Force	Page Overlays	Imposter QR	Gift Cards	
Public Domain	Infected ATM	Loyalty Programs	Social Media	Session Cookie Capture	Session Hijack	Fake Extensions	NFC Payments	NFC Relay (Token Relay)	
Dark Web	SIP Services	Official Phone Number Spoofing	Message	HTTPS Intercept	Remote Access	2FA Compromise	Stolen Card Use	Crypto Purchase	
	Malvertising	Profitable Propositions	Scam Ads	Illegal Access to Database	Virtual Machines	Malware	Network Interception		
	App Repackaging	Employee Credentials	Fake Support	Password Stealer		Caller ID Spoofing	Mule Card Transfers		
	Malware	Employee Impersonation	Fake Call Centers	Phone Number Disclosure			Bonus Withdrawal		
	Supply Chain Compromise	Account Detail Changes	Fake (Merchant) Websites	Man in the Middle			ATM Jackpotting		
	Fake Accounts	Branded Resources	Fake Apps	Fake Forms			Shipping Redirect		
	Hosting Services	Website Redirects					Payments from Mule Account		
	Money Mules	Prepaid Reservations					Payment to Mule Account		
		Payment via Gift Card							
		Social Engineering							

Digital Wallet Attacks: Preparation of the MOs

Resource Development	Psychological Manipulation	Faux Communications
Acquire Infrastructure	Romance	Phishing
Compromise Infrastructure	Impersonation	Spearphishing
Social Networks Accounts	Accessibility Permissions	Smishing
Infected POS	Fake Loan Requests	Vishing
Infected ATM	Loyalty Programs	Social Media
SIP Services	Official Phone Number Spoofing	Message
Malvertising	Profitable Propositions	Scam Ads
App Repackaging	Employee Credentials	Fake Support
Malware	Employee Impersonation	Fake Call Centers
Supply Chain Compromise	Account Detail Changes	Fake (Merchant) Websites
Fake Accounts	Branded Resources	Fake Apps
Hosting Services	Website Redirects	
Money Mules	Prepaid Reservations	
	Payment via Gift Card	
	Social Engineering	

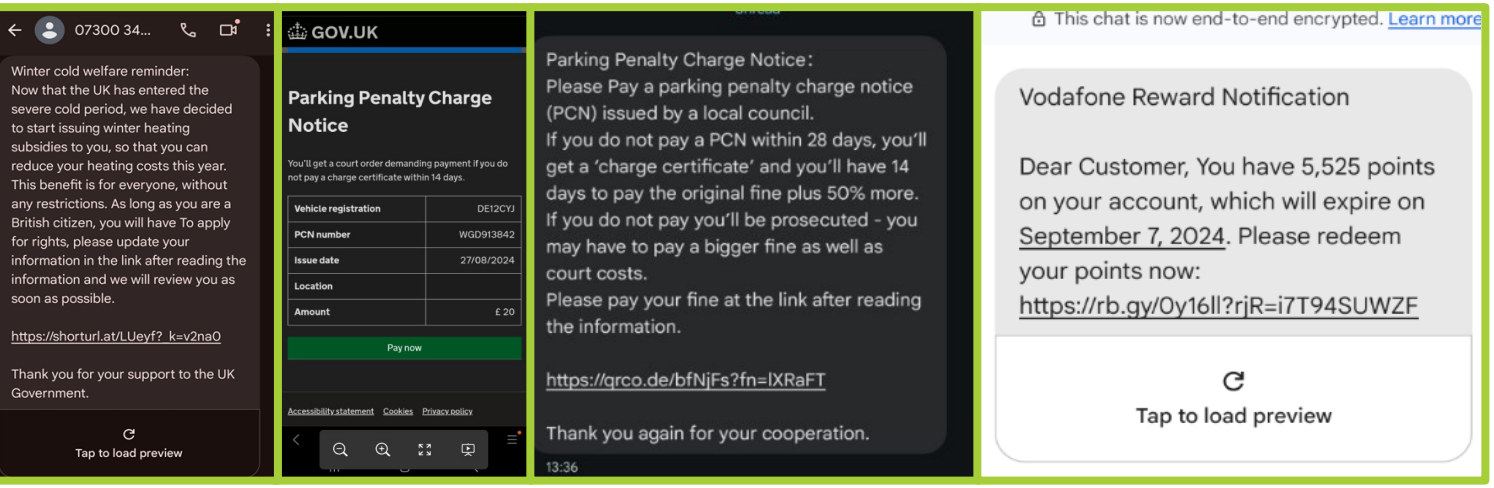

+63 968 448 6920
iMessage
Today 1:34 PM
Your toll payment for TxTag Lane must be settled by March 24, 2025. To avoid fines and the suspension of your driving privileges, kindly pay by the due date.
Pay here:https://txtag.epdtk.shop/pay
(Please reply with "Y," then exit the text message. Open it again, click the link, or copy it into your Safari browser and open it.)
The sender is not in your contact list.
Report Junk
IDAHO DMV Final Reminder:
You have an outstanding toll.Your toll account balance is outstanding. If you fail to pay by March 24, 2025. You will be penalized or subject to legal action.
Now Payment:
https://dmvonline.gvo-idetsh.cc/us
(Please reply Y, then exit the SMS and open it again to activate the link, or copy the link to your Safari browser and open it)
Please settle your toll immediately after reading this message to avoid penalties for delaying the payment.
Thank you for your cooperation.
E-ZPass Final Reminder:
You have an outstanding toll.Your toll account balance is outstanding. If you fail to pay by March 24, 2025. You will be penalized or subject to legal action.
Now Payment:
https://ezpass.com-etcmt.xin/us
(Please reply Y, then exit the SMS and open it again to activate the link, or copy the link to your Safari browser and open it)
Please settle your toll immediately after reading this message to avoid penalties for delaying the payment.
Thank you for your cooperation.
(567) 435-3688
Save (567) 435-3688?
Saving this number will add a new contact
Report spam
Add contact
This chat is now end-to-end encrypted. Learn more
Unread
Urgent: Avoid Costly Penalties on Ur Toll Fees
Ur toll balance is still unpaid. You must settle it by March 25, 2025, or you risk:
Suspended vehicle registration
Higher fines
Damage to ur credit score
https://shorturl.at/q8QJZ?MCG=6585ds4j
Act now before penalties increase!
0324-952973F1D52749954
Tap to load preview
7:03 AM
RCS message
E-ZPass Final Reminder:
You have an outstanding toll.Your toll account balance is outstanding. If you fail to pay by March 25, 2025. You will be penalized or subject to legal action.
Now Payment:
https://e-zpassny.com-wxl.vip/us
(Please reply Y, then exit the SMS and open it again to activate the link, or copy the link to your Safari browser and open it)
Please settle your toll immediately after reading this message to avoid penalties for delaying the payment.
Thank you for your cooperation.

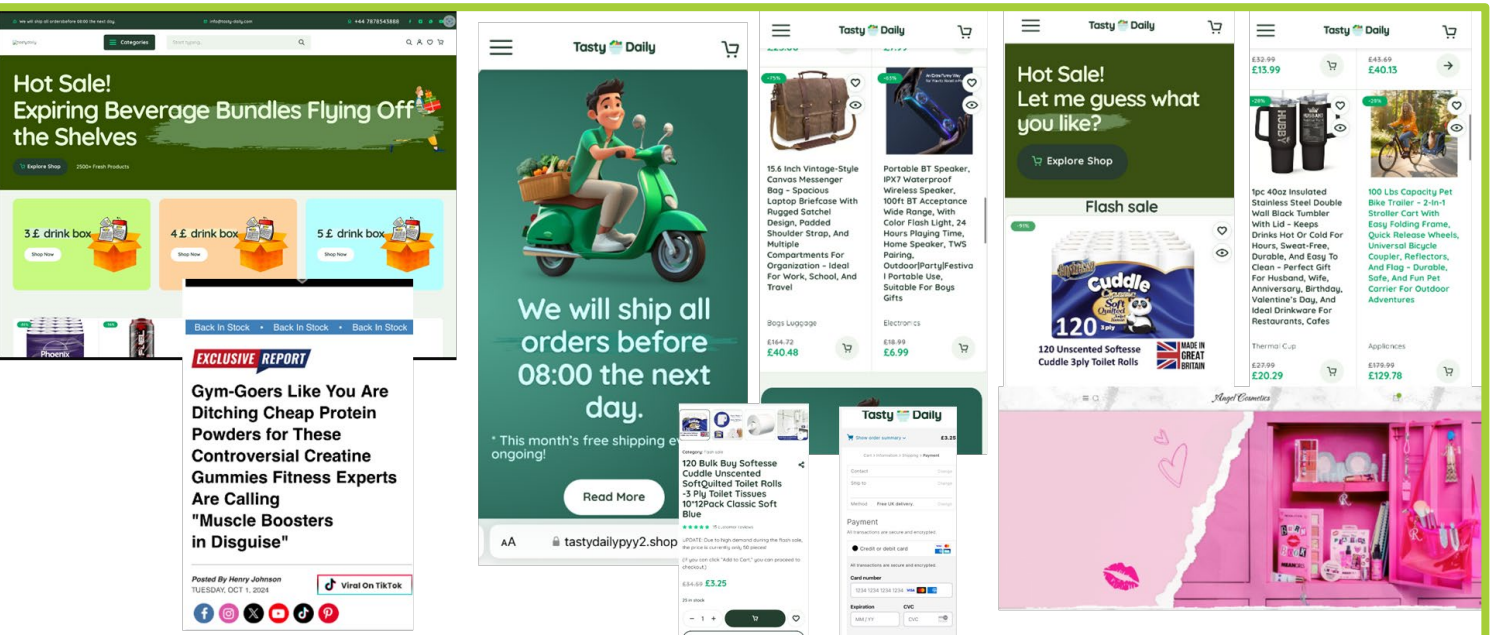


BARCLAYS THREAT FABRIC

RSAC 2025 Conference

Digital Wallet Attacks: Preparation of the MOs


07300 34...
Winter cold welfare reminder:
Now that the UK has entered the severe cold period, we have decided to start issuing winter heating subsidies to you, so that you can reduce your heating costs this year. This benefit is for everyone, without any restrictions. As long as you are a British citizen, you will have To apply for rights, please update your information in the link after reading the information and we will review you as soon as possible.
https://shorturl.at/LUeyf?_k=v2na0
Thank you for your support to the UK Government.
Tap to load preview
GOV.UK
Parking Penalty Charge Notice
You'll get a court order demanding payment if you do not pay a charge certificate within 14 days.
Vehicle registration DE12CYJ
PCN number WGD913842
Issue date 27/08/2024
Location
Amount £ 20
Pay now
Accessibility statement Cookies Privacy policy
Parking Penalty Charge Notice:
Please Pay a parking penalty charge notice (PCN) issued by a local council.
If you do not pay a PCN within 28 days, you'll get a 'charge certificate' and you'll have 14 days to pay the original fine plus 50% more.
If you do not pay you'll be prosecuted - you may have to pay a bigger fine as well as court costs.
Please pay your fine at the link after reading the information.
https://qrco.de/bfNjFs?fn=IXRaFT
Thank you again for your cooperation.
13:36
This chat is now end-to-end encrypted. Learn more
Vodafone Reward Notification
Dear Customer, You have 5,525 points on your account, which will expire on September 7, 2024. Please redeem your points now:
https://rb.gy/0y16ll?rjR=i7T94SUWZF
Tap to load preview


Hot Sale!
Expiring Beverage Bundles Flying Off the Shelves
3£ drink box
4£ drink box
5£ drink box
Back In Stock • Back In Stock • Back In Stock
EXCLUSIVE REPORT
Gym-Goers Like You Are Ditching Cheap Protein Powders for These Controversial Creatine Gummies Fitness Experts Are Calling "Muscle Boosters in Disguise"
Posted By Henry Johnson
TUESDAY, OCT 1, 2024
Viral On TikTok
Tasty Daily
We will ship all orders before 08:00 the next day.
* This month's free shipping ongoing!
Read More
tastydailypyy2.shop
120 Bulk Buy Softesse Cuddle Unscented SoftQuilted Toilet Rolls -3 Ply Toilet Tissues 10*12Pack Classic Soft Blue
£3.25
Hot Sale!
Let me guess what you like?
Explore Shop
Flash sale
120 Unscented Softesse Cuddle 3ply Toilet Rolls
£20.29
£129.78

Threat actor group A (TAGA) sets up a Crime-as-a-Service (CaaS) model for purchase of custom phishing kits & admin panel.

Phishing urls often set up behind CloudFlare and use IP Whitelisting and other access restrictions

TAGA advertise their service for sale on platforms such as telegram, with tutorials

Threat actor Group B(TAGB) purchase use of the Phishing-as-a-Service and/or Smishing-as-a-Service + tutorials

TAGB deploys the phish kits via the fake advertisements or sends via SMS in mass using smishing farms.

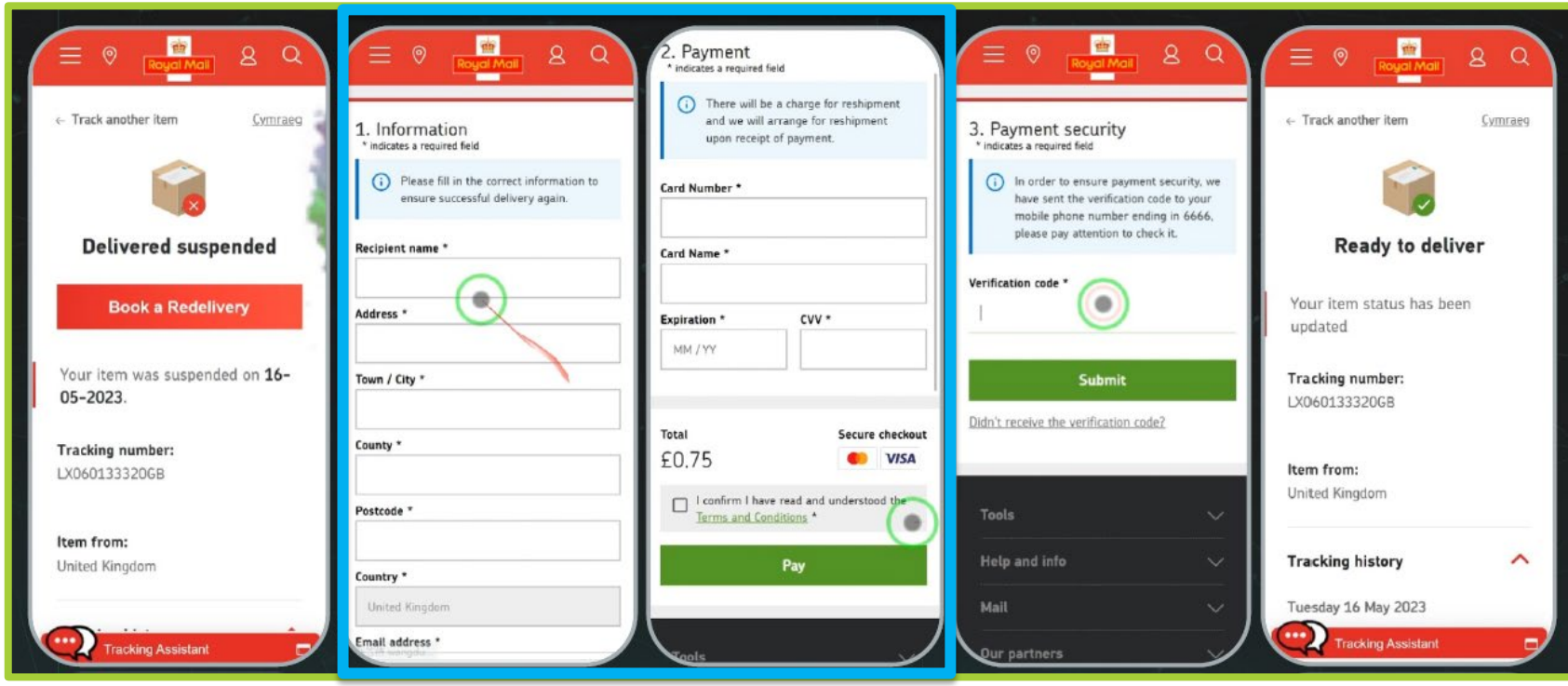
Phish Kit Admin Panels enable the threat actor to see compromised victim data come through in real time.

Digital Wallet Attacks: Compromise

Reconnaissance	Resource Development	Psychological Manipulation	Faux Communications	Credential Compromise	Account Access	Authorization Compromise	Fraud Event	Monetization	Money Laundering
SMS Intercept	Acquire Infrastructure	Romance	Phishing	Keyloggers	Device Compromise	Location Spoofing	Victim Transfer	Cashout	Resale of Goods
Bots	Compromise Infrastructure	Impersonation	Spearphishing	Screen Capture	Insiders	Virtual Phone	Account Takeover	Subscriptions	Crypto Mixers
Malware	Social Networks Accounts	Accessibility Permissions	Smishing	SMS Intercept	Cloned Devices	Voice Changers	P2P Transfers	ATM Withdrawal	
Personal Info	Infected POS	Fake Loan Requests	Vishing	Card Dump Captures	Brute Force	Page Overlays	Imposter QR	Gift Cards	
Public Domain	Infected ATM	Loyalty Programs	Social Media	Session Cookie Capture	Session Hijack	Fake Extensions	NFC Payments	NFC Relay (Token Relay)	
Dark Web	SIP Services	Official Phone Number Spoofing	Message	HTTPS Intercept	Remote Access	2FA Compromise	Stolen Card Use	Crypto Purchase	
	Malvertising	Profitable Propositions	Scam Ads	Illegal Access to Database	Virtual Machines	Malware	Network Interception		
	App Repackaging	Employee Credentials	Fake Support	Password Stealer		Caller ID Spoofing	Mule Card Transfers		
	Malware	Employee Impersonation	Fake Call Centers	Phone Number Disclosure			Bonus Withdrawal		
	Supply Chain Compromise	Account Detail Changes	Fake (Merchant) Websites	Man in the Middle			ATM Jackpotting		
	Fake Accounts	Branded Resources	Fake Apps	Fake Forms			Shipping Redirect		
	Hosting Services	Website Redirects					Payments from Mule Account		
	Money Mules	Prepaid Reservations					Payment to Mule Account		
		Payment via Gift Card							
		Social Engineering							

Digital Wallet Attacks: Compromise

Psychological Manipulation	Faux Communications	Credential Compromise
Romance	Phishing	Keyloggers
Impersonation	Spearphishing	Screen Capture
Accessibility Permissions	Smishing	SMS Intercept
Fake Loan Requests	Vishing	Card Dump Captures
Loyalty Programs	Social Media	Session Cookie Capture
Official Phone Number Spoofing	Message	HTTPS Intercept
Profitable Propositions	Scam Ads	Illegal Access to Database
Employee Credentials	Fake Support	Password Stealer
Employee Impersonation	Fake Call Centers	Phone Number Disclosure
Account Detail Changes	Fake (Merchant) Websites	Man in the Middle
Branded Resources	Fake Apps	Fake Forms
Website Redirects		
Prepaid Reservations		
Payment via Gift Card		
Social Engineering		



Digital Wallet Attacks: Access

Reconnaissance	Resource Development	Psychological Manipulation	Faux Communications	Credential Compromise	Account Access	Authorization Compromise	Fraud Event	Monetization	Money Laundering
SMS Intercept	Acquire Infrastructure	Romance	Phishing	Keyloggers	Device Compromise	Location Spoofing	Victim Transfer	Cashout	Resale of Goods
Bots	Compromise Infrastructure	Impersonation	Spearphishing	Screen Capture	Insiders	Virtual Phone	Account Takeover	Subscriptions	Crypto Mixers
Malware	Social Networks Accounts	Accessibility Permissions	Smishing	SMS Intercept	Cloned Devices	Voice Changers	P2P Transfers	ATM Withdrawal	
Personal Info	Infected POS	Fake Loan Requests	Vishing	Card Dump Captures	Brute Force	Page Overlays	Imposter QR	Gift Cards	
Public Domain	Infected ATM	Loyalty Programs	Social Media	Session Cookie Capture	Session Hijack	Fake Extensions	NFC Payments	NFC Relay (Token Relay)	
Dark Web	SIP Services	Official Phone Number Spoofing	Message	HTTPS Intercept	Remote Access	2FA Compromise	Stolen Card Use	Crypto Purchase	
	Malvertising	Profitable Propositions	Scam Ads	Illegal Access to Database	Virtual Machines	Malware	Network Interception		
	App Repackaging	Employee Credentials	Fake Support	Password Stealer		Caller ID Spoofing	Mule Card Transfers		
	Malware	Employee Impersonation	Fake Call Centers	Phone Number Disclosure			Bonus Withdrawal		
	Supply Chain Compromise	Account Detail Changes	Fake (Merchant) Websites	Man in the Middle			ATM Jackpotting		
	Fake Accounts	Branded Resources	Fake Apps	Fake Forms			Shipping Redirect		
	Hosting Services	Website Redirects					Payments from Mule Account		
	Money Mules	Prepaid Reservations					Payment to Mule Account		
		Payment via Gift Card							
		Social Engineering							

Digital Wallet Attacks: Access

Credential Compromise	Account Access	Authorization Compromise	Fraud Event
Keyloggers	Device Compromise	Location Spoofing	Victim Transfer
Screen Capture	Insiders	Virtual Phone	Account Takeover
SMS Intercept	Cloned Devices	Voice Changers	P2P Transfers
Card Dump Captures	Brute Force	Page Overlays	Imposter QR
Session Cookie Capture	Session Hijack	Fake Extensions	NFC Payments
HTTPS Intercept	Remote Access	2FA Compromise	Stolen Card Use
Illegal Access to Database	Virtual Machines	Malware	Network Interception
Password Stealer		Caller ID Spoofing	Mule Card Transfers
Phone Number Disclosure			Bonus Withdrawal
Man in the Middle			ATM Jackpotting
Fake Forms			Shipping Redirect
			Payments from Mule Account
			Payment to Mule Account

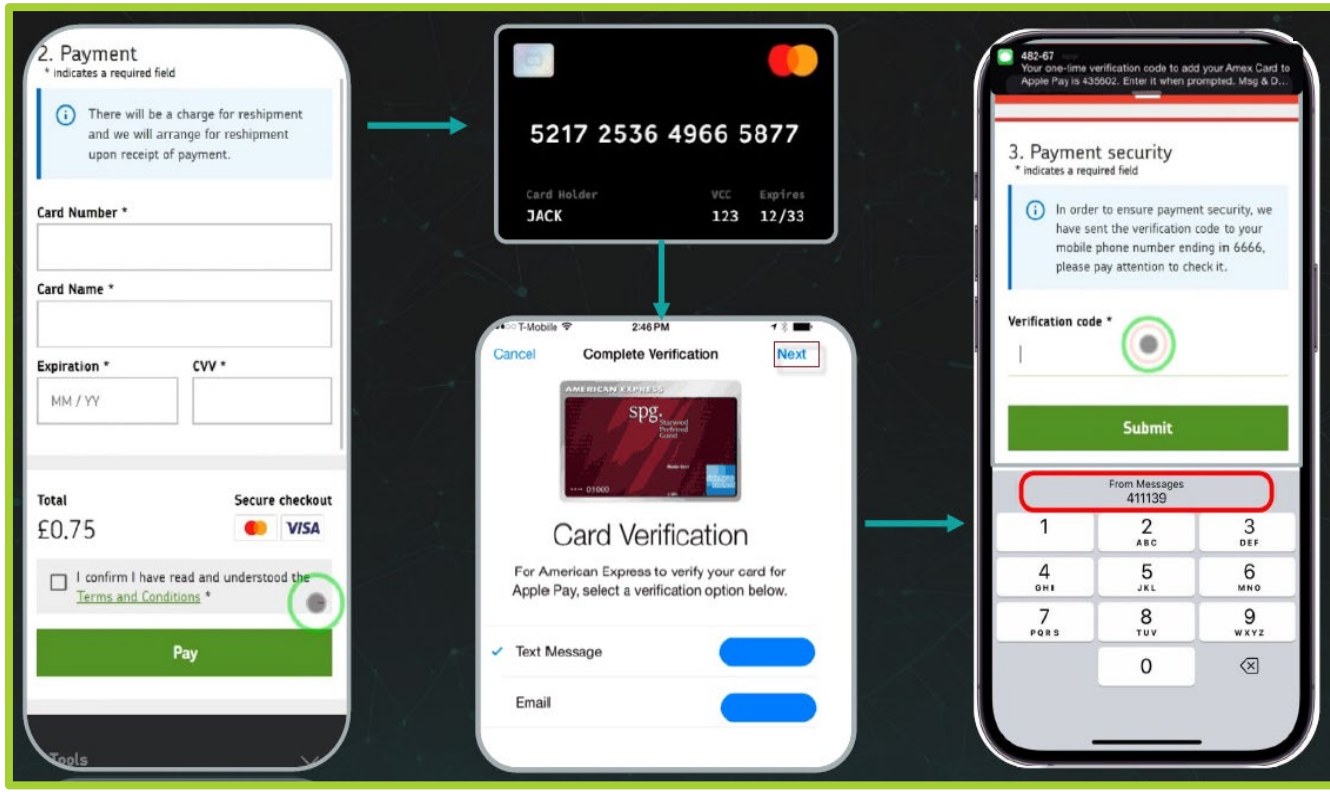
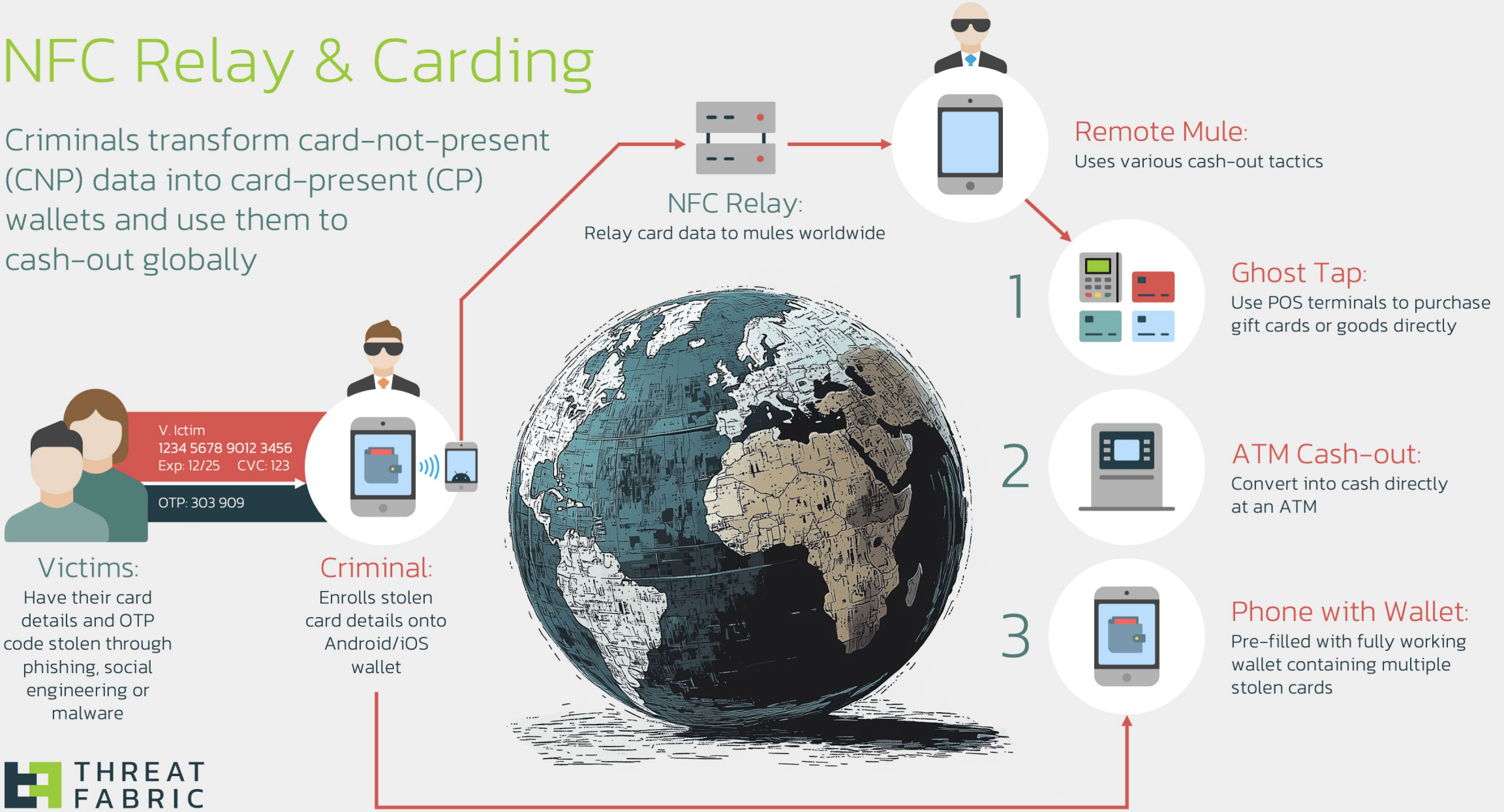


Image source: krebsonsecurity.com

NFC Relay & Carding

Criminals transform card-not-present (CNP) data into card-present (CP) wallets and use them to cash-out globally



Victims:

Have their card details and OTP code stolen through phishing, social engineering or malware

Criminal:

Enrolls stolen card details onto Android/iOS wallet

NFC Relay:

Relay card data to mules worldwide

Remote Mule:

Uses various cash-out tactics

1

Ghost Tap:

Use POS terminals to purchase gift cards or goods directly

2

ATM Cash-out:

Convert into cash directly at an ATM

3

Phone with Wallet:

Pre-filled with fully working wallet containing multiple stolen cards

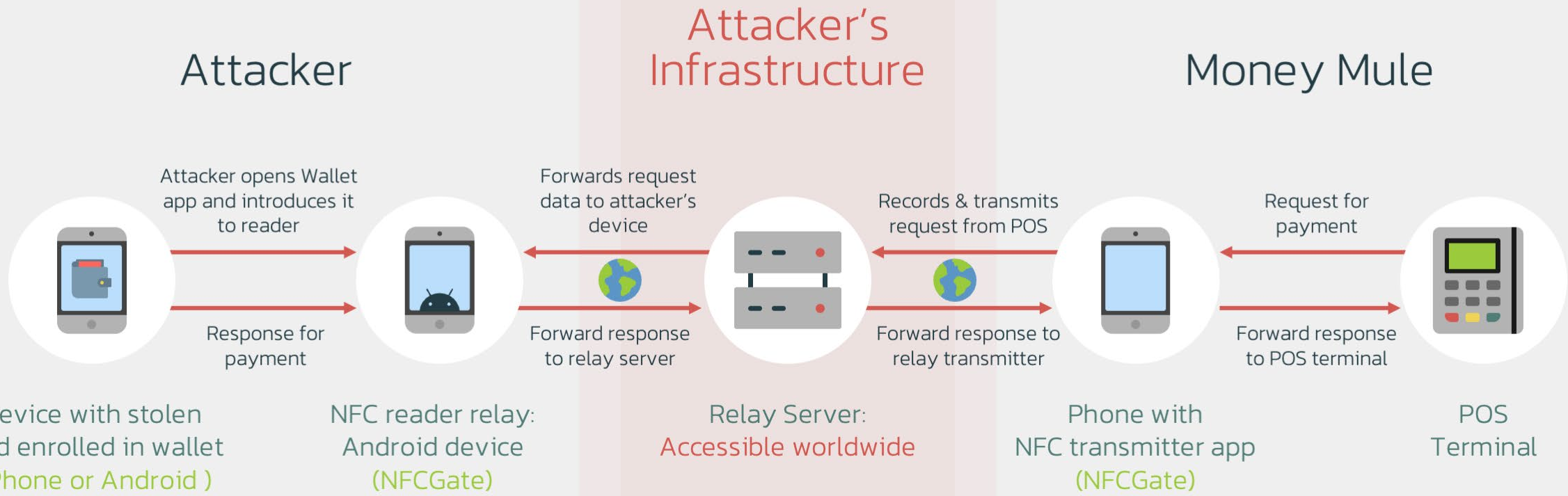
THREAT FABRIC

Digital Wallet Attacks: NFC Relay

Reconnaissance	Resource Development	Psychological Manipulation	Faux Communications	Credential Compromise	Account Access	Authorization Compromise	Fraud Event	Monetization	Money Laundering
SMS Intercept	Acquire Infrastructure	Romance	Phishing	Keyloggers	Device Compromise	Location Spoofing	Victim Transfer	Cashout	Resale of Goods
Bots	Compromise Infrastructure	Impersonation	Spearphishing	Screen Capture	Insiders	Virtual Phone	Account Takeover	Subscriptions	Crypto Mixers
Malware	Social Networks Accounts	Accessibility Permissions	Smishing	SMS Intercept	Cloned Devices	Voice Changers	P2P Transfers	ATM Withdrawal	
Personal Info	Infected POS	Fake Loan Requests	Vishing	Card Dump Captures	Brute Force	Page Overlays	Imposter QR	Gift Cards	
Public Domain	Infected ATM	Loyalty Programs		Session Cookie Capture	Session Hijack		NFC Payments	NFC Relay (Token Relay)	
Dark Web	SIP Services	Official Phone Number Spoofing	Message		Remote Access	2FA Compromise	Stolen Card Use	Crypto Purchase	
	Malvertising	Profitable Propositions			Virtual Machines		Network Interception		
	App Repackaging	Employee Credentials	Fake Support	Illegal Access to		Caller ID Spoofing	Mule Card Transfers		
	Malware	Employee Impersonation	Fake Call Centers	Phone Number Disclosure			Bonus Withdrawal		
	Supply Chain Compromise	Account Detail Changes	Fake Apps	Man in the Middle			ATM Jackpotting		
	Fake Accounts	Branded Resources		Fake Forms			Shipping Redirect		
	Hosting Services	Website Redirects					Payments from Mule Account		
	Money Mules	Prepaid Reservations					Payment to Mule Account		
		Payment via Gift Card							
		Social Engineering							

It's the first time we've seen such widespread misuse of the mobile "on the right side" of the Fraud Kill Chain

Cash-out with NFC Relay

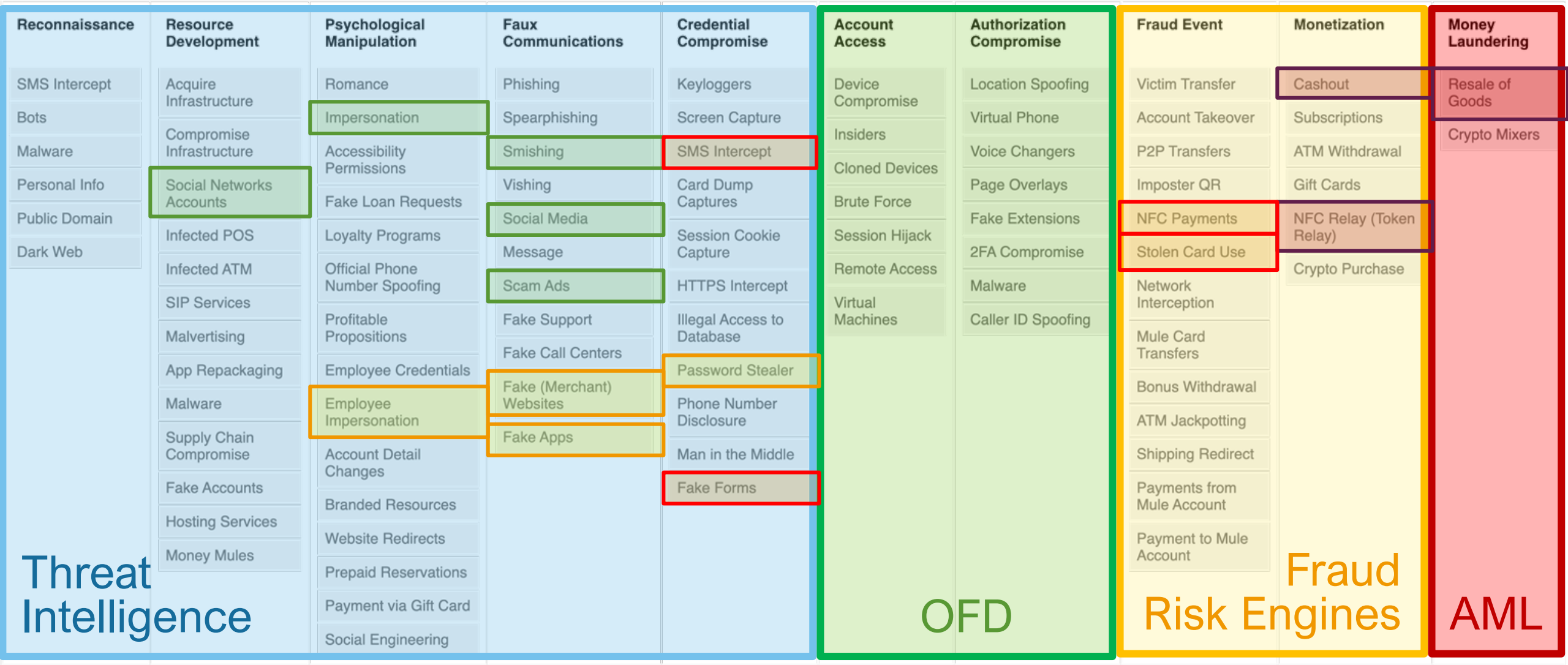

Attacker
Attacker's Infrastructure
Money Mule
Attacker opens Wallet app and introduces it to reader
Response for payment
Forwards request data to attacker's device
Forward response to relay server
Records & transmits request from POS
Forward response to relay transmitter
Request for payment
Forward response to POS terminal
Device with stolen card enrolled in wallet (iPhone or Android)
NFC reader relay: Android device (NFCGate)
Relay Server: Accessible worldwide
Phone with NFC transmitter app (NFCGate)
POS Terminal

THREAT FABRIC

Digital Wallet Attacks: all TTPs

Reconnaissance	Resource Development	Psychological Manipulation	Faux Communications	Credential Compromise	Account Access	Authorization Compromise	Fraud Event	Monetization	Money Laundering
SMS Intercept	Acquire Infrastructure	Romance	Phishing	Keyloggers	Device Compromise	Location Spoofing	Victim Transfer	Cashout	Resale of Goods
Bots	Compromise Infrastructure	Impersonation	Spearphishing	Screen Capture	Insiders	Virtual Phone	Account Takeover	Subscriptions	Crypto Mixers
Malware	Social Networks Accounts	Accessibility Permissions	Smishing	SMS Intercept	Cloned Devices	Voice Changers	P2P Transfers	ATM Withdrawal	
Personal Info	Infected POS	Fake Loan Requests	Vishing	Card Dump Captures	Brute Force	Page Overlays	Imposter QR	Gift Cards	
Public Domain	Infected ATM	Loyalty Programs	Social Media	Session Cookie Capture	Session Hijack	Fake Extensions	NFC Payments	NFC Relay (Token Relay)	
Dark Web	SIP Services	Official Phone Number Spoofing	Message	HTTPS Intercept	Remote Access	2FA Compromise	Stolen Card Use	Crypto Purchase	
	Malvertising	Profitable Propositions	Scam Ads	Illegal Access to Database	Virtual Machines	Malware	Network Interception		
	App Repackaging	Employee Credentials	Fake Support	Password Stealer		Caller ID Spoofing	Mule Card Transfers		
	Malware	Employee Impersonation	Fake Call Centers	Phone Number Disclosure			Bonus Withdrawal		
	Supply Chain Compromise	Account Detail Changes	Fake (Merchant) Websites	Man in the Middle			ATM Jackpotting		
	Fake Accounts	Branded Resources	Fake Apps	Fake Forms			Shipping Redirect		
	Hosting Services	Website Redirects					Payments from Mule Account		
	Money Mules	Prepaid Reservations					Payment to Mule Account		
		Payment via Gift Card							
		Social Engineering							

Digital Wallet Attacks: Mitigation



BARCLAYS THREAT FABRIC

RSAC 2025 Conference

Digital Wallet Attacks: Mitigation

Reconnaissance	Resource Development	Psychological Manipulation	Faux Communications	Credential Compromise	Account Access	Authorization Compromise	Fraud Event	Monetization	Money Laundering

Threat Intelligence

- Phishing Hunt/Detection
- Telco Intel Sharing & Blocking
- ISP/Browser Intel Sharing & Blocking
- Social Media Co. Collaboration
- Scheme Collaboration
- Apple/Google Collaboration
- Law Enforcement Disruption
- Device Level Smishing Blocks
- Threat Intelligence Collection & Validation
- Law Enforcement / Industry Intel Sharing
- Merchant IDs (online, POS and ACTO)
- SEIDs

OFD

Fraud Risk Engines

- 1st transactions on new token
- New transactions within 90 days
- Look for ‘impossible spends’
- Created/used fraudulently: consider card compromised

AML

BARCLAYS THREAT FABRIC

Enhance digital wallet provisioning journey

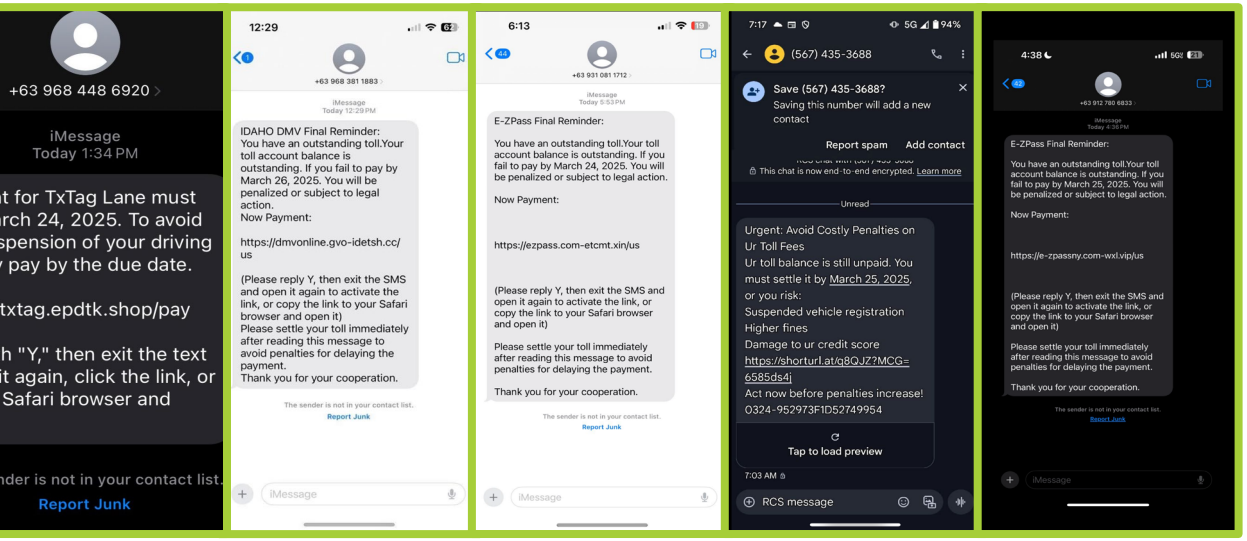
Incorporate CP data in Risk Engines

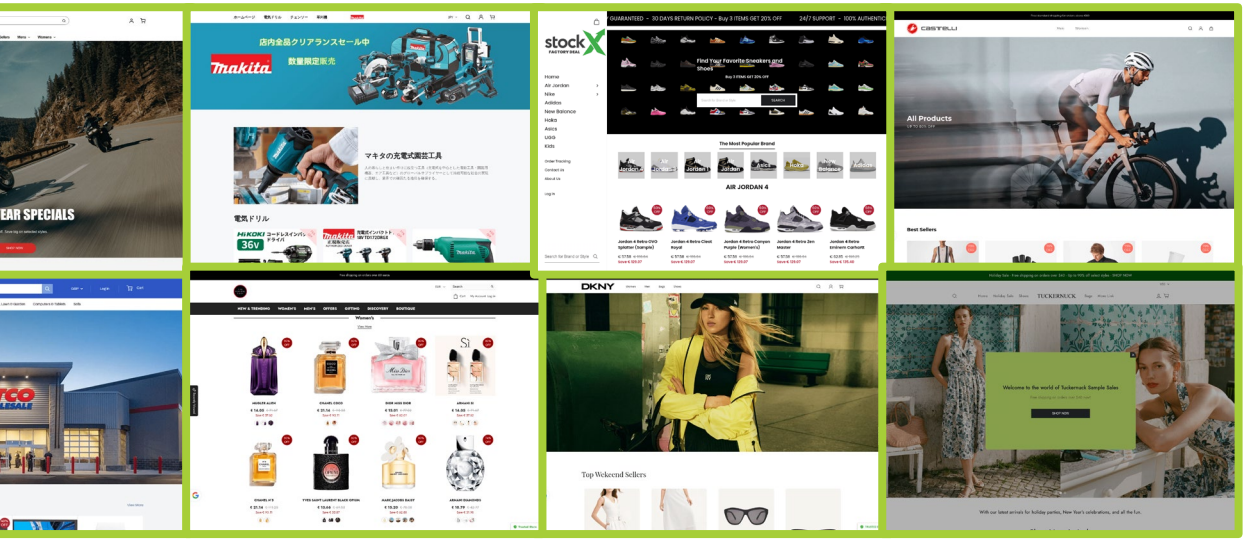
- Device location <-> cardholders' residence or work / recent transaction sites.
- Recent online banking app activation/activity
- Name, address and CVC2 matching
- Recent account changes (telephone number / email address)

Inform, push & avoid

- Inform Cardholders of new provisioning, & new transactions (In-App, Email, SMS)
- “Push Provisioning”
- Avoid SMS OTP

Apply: Digital Wallet Attacks


+63 968 448 6920
iMessage
Today 1:34 PM
Report Junk
12:29
IDAHO DMV Final Reminder:
You have an outstanding toll.Your toll account balance is outstanding. If you fail to pay by March 26, 2025. You will be penalized or subject to legal action.
Now Payment:
https://dmvonline.gvo-idetsh.cc/us
(Please reply Y, then exit the SMS and open it again to activate the link, or copy the link to your Safari browser and open it)
Please settle your toll immediately after reading this message to avoid penalties for delaying the payment.
Thank you for your cooperation.
6:13
E-ZPass Final Reminder:
You have an outstanding toll.Your toll account balance is outstanding. If you fail to pay by March 24, 2025. You will be penalized or subject to legal action.
Now Payment:
https://ezpass.com-etcmt.xin/us
(Please reply Y, then exit the SMS and open it again to activate the link, or copy the link to your Safari browser and open it)
Please settle your toll immediately after reading this message to avoid penalties for delaying the payment.
Thank you for your cooperation.
7:17
(567) 435-3688
Save (567) 435-3688?
Saving this number will add a new contact
Report spam
Add contact
This chat is now end-to-end encrypted. Learn more
Unread
Urgent: Avoid Costly Penalties on Ur Toll Fees
Ur toll balance is still unpaid. You must settle it by March 25, 2025, or you risk:
Suspended vehicle registration
Higher fines
Damage to ur credit score
https://shorturl.at/q8QJZ?MCG=6585ds4j
Act now before penalties increase!
0324-952973F1D52749954
Tap to load preview
7:03 AM
RCS message
4:38
E-ZPass Final Reminder:
You have an outstanding toll.Your toll account balance is outstanding. If you fail to pay by March 25, 2025. You will be penalized or subject to legal action.
Now Payment:
https://e-zpassny.com-wxl.vip/us
(Please reply Y, then exit the SMS and open it again to activate the link, or copy the link to your Safari browser and open it)
Please settle your toll immediately after reading this message to avoid penalties for delaying the payment.
Thank you for your cooperation.



Digital Wallet Attacks

- Carding has “returned”
- It misuses Card Not Present data in Card Present Fraud
- Multiple Cashout methods, including NFC relaying
- Because of this, for Many FIs it’s hard to detect (no CNP capabilities on CP channels)
- Collaboration with Telcos, Apple, Google & Social Media is key
- Provisioning Journey should be enhanced

Fraud Kill Chain: “Drifting Together”

Call to Collaborate!

- We know we’re not the only show in town…
- ISACs, Retail, Banking Associations are working on Structuring Fraud MO Processes.
- Our aim – by publishing our work, collaboration and consolidation of ideas will happen
- Let’s “Drift Together” – not “Drifting Apart”

Apply: Fraud Kill Chain

Fraud Kill Chain

- Fraud Prevention needs a shared vocabulary & common framework
- The Fraud Kill Chain allows for financial events & behavioral TTPs
- It crosses the chasm between Threat Intelligence & Fraud Prevention teams & who knows… even AML
- We decided to open our work. So today we're launching…

fraudkillchain.com

FKC.

Explore the Fraud Kill Chain Contact

The Fraud Kill Chain

Real-world examples

Select a threat:

None | Device Takeover (DTO) | Romance Scam | Investment Scam | Anatsa (malware) | Digital Wallet Attack

Reconnaissance	Resource Development	Psychological Manipulation	Faux Communications	Credential Compromise	Account Access	Authorization Compromise	Fraud Event	Monetization	Money Laundering
SMS Intercept	Acquire Infrastructure	Romance	Phishing	Keyloggers	Device Compromise	Location Spoofing	Victim Transfer	Cashout	Resale of Goods
Bots	Compromise Infrastructure	Impersonation	Spearphishing	Screen Capture	Insiders	Virtual Phone	Account Takeover	Subscriptions	Crypto Mixers
Malware	Social Networks Accounts	Accessibility Permissions	Smishing	SMS Intercept	Cloned Devices	Voice Changers	P2P Transfers	ATM Withdrawal	
Personal Info	Infected POS	Fake Loan Requests	Vishing	Card Dump Captures	Brute Force	Page Overlays	Imposter QR	Gift Cards	
Public Domain	Infected ATM	Loyalty Programs	Social Media	Session Cookie Capture	Session Hijack	Fake Extensions	NFC Payments	NFC Relay (Token Relay)	
Dark Web	SIP Services	Official Phone Number Spoofing	Message	HTTPS Intercept	Remote Access	2FA Compromise	Stolen Card Use	Crypto Purchase	
	Malvertising	Profitable Propositions	Scam Ads	Illegal Access to Database	Virtual Machines	Malware	Network Interception		

Shout-outs

- CSIS
- Brian Krebs
- Law enforcement: first arrests made End of March!

BARCLAYS THREAT FABRIC

RSAC 2025 Conference

Many Voices.
One Community.

Thank you!

Senan: https://www.linkedin.com/in/senan-moloney-9600053b

Eward: https://www.linkedin.com/in/ewarddriehuis

www.fraudkillchain.com
www.threatfabric.com